

Quantum discord and the power of one qubit

Animesh Datta,* Anil Shaji,[†] and Carlton M. Caves

Department of Physics and Astronomy, MSC07-4220, 1 University of New Mexico, Albuquerque, New Mexico 87131-0001

(Dated: February 1, 2008)

We use quantum discord to characterize the correlations present in the quantum computational model DQC1, introduced by Knill and Laflamme [Phys. Rev. Lett. **81**, 5672 (1998)]. The model involves a collection of qubits in the completely mixed state coupled to a single control qubit that has nonzero purity. The initial state, operations, and measurements in the model all point to a natural bipartite split between the control qubit and the mixed ones. Although there is no entanglement between these two parts, we show that the quantum discord across this split is nonzero for typical instances of the DQC1 circuit. Nonzero values of discord indicate the presence of nonclassical correlations. We propose quantum discord as figure of merit for characterizing the resources present in this computational model.

PACS numbers: 03.67.-a, 03.65.Ud,

Keywords: Quantum Discord, DQC1

Characterizing and quantifying the information-processing capabilities offered by quantum phenomena like entanglement, superposition, and interference is one of the primary objectives of quantum information theory. In spite of substantial progress [1, 2, 3], the precise role of entanglement in quantum information processing remains an open question [4, 5, 6, 7, 8, 9]. It is quite well established that entanglement is essential for certain kinds of quantum-information tasks like quantum cryptography and super-dense coding. In these cases, it is also known that the quantum enhancement must come from entanglement spread over large parts of the system. It is not known, however, if all information-processing tasks that can be done more efficiently with a quantum system than with a comparable classical system require entanglement as a resource.

For pure-state quantum computation, it is known that entanglement must grow with the system size for there to be exponential speedup [2]. There is evidence that quantum information processors using highly mixed states, with no discernible entanglement, can perform better [5, 7, 8, 10] than equivalent classical ones. Indeed, there exist models of mixed-state quantum computation that provide exponential speedup over the best known classical algorithms and yet have a bounded amount of entanglement [11]. Here we explore an alternate way of characterizing the quantum nature of the correlations in such systems.

Quantum discord, introduced by Ollivier and Zurek and independently by Henderson and Vedral [12, 13], captures the nonclassical correlations, including but not limited to entanglement, that can exist between parts of a quantum system. We investigate the effectiveness of discord in characterizing the performance of the model of quantum information processing introduced by Knill and Laflamme in [11], which is often referred to as the *power of one qubit*, or DQC1. In this model, information processing is performed with a collection of qubits in the completely mixed state coupled to a single control qubit that has some nonzero purity. Such a device can perform efficiently certain computational tasks for which there is no known efficient method using classical information

processors.

We start with a discussion of quantum discord, its definition and its relevance in quantum information theory. Consider the following two-qubit separable state

$$\rho = \frac{1}{4} \left(|+\rangle\langle+| \otimes |0\rangle\langle 0| + |-\rangle\langle-| \otimes |1\rangle\langle 1| + |0\rangle\langle 0| \otimes |-\rangle\langle-| + |1\rangle\langle 1| \otimes |+\rangle\langle+| \right), \quad (1)$$

in which four nonorthogonal states of the first qubit are correlated with four nonorthogonal states of the second qubit. Such correlations cannot exist in any classical state of two bits. The extra correlations the quantum state can contain compared to an equivalent classical system with two bits could reasonably be called quantum correlations. Entanglement is a special kind of quantum correlation, but not the only kind. In other words, separable quantum states can have correlations that cannot be captured by a probability distribution defined over the states of an equivalent classical system.

Quantum discord attempts to quantify all quantum correlations including entanglement. It must be emphasized here that the discord, in a sense, supplements the measures of entanglement that can be defined on the system of interest. It aims to capture all the nonclassical correlations present in a system, those that can be identified as entanglement and then some more.

The information-theoretic measure of correlations between two systems S and M is the mutual information,

$$\mathcal{I}(S : M) = H(S) + H(M) - H(S, M). \quad (2)$$

If M and S are classical systems whose state is described by a probability distribution $p(S, M)$, then $H(\cdot)$ denotes the Shannon entropy, $H(\vec{p}) \equiv -\sum_j p_j \log p_j$. If M and S are quantum systems described by a combined density matrix ρ_{SM} , then $H(\cdot)$ stands for the corresponding von Neumann entropy, $H(\rho) \equiv -\text{Tr}(\rho \log \rho)$.

For classical probability distributions, Bayes's rule leads to an equivalent expression for the mutual information,

$$\mathcal{I}(S : M) = H(S) - H(S|M), \quad (3)$$

where the conditional entropy $H(S|M)$ is an average of Shannon entropies for S , conditioned on the alternatives for M . For quantum systems, we can regard Eq. (3) as defining a conditional entropy, but it is not an average of von Neumann entropies and is not necessarily nonnegative [14].

Another way of generalizing the classical conditional entropy to the quantum case is to recognize that classically $H(S|M)$ quantifies the ignorance about the system S that remains if we make measurements to determine M . When M is a quantum system, the amount of information we can extract about it depends on the choice of measurement. If we restrict to projective measurements described by a complete set of orthogonal projectors, $\{\Pi_j\}$, corresponding to outcomes j , then the state of S after a measurement is given by

$$\rho_{S|j} = \frac{\text{Tr}_M(\Pi_j \rho_{SM} \Pi_j)}{p_j}, \quad p_j = \text{Tr}_{S,M}(\rho_{SM} \Pi_j). \quad (4)$$

A quantum analogue of the conditional entropy can then be defined as $\tilde{H}_{\{\Pi_j\}}(S|M) \equiv \sum_j p_j H(\rho_{S|j}) \geq 0$. Since $\rho_S = \sum_j p_j \rho_{S|j}$, the concavity of von Neumann entropy implies that $H(S) \geq \tilde{H}_{\{\Pi_j\}}(S|M)$. We can now define an alternative quantum version of the mutual information,

$$\mathcal{J}_{\{\Pi_j\}}(S : M) \equiv H(S) - \tilde{H}_{\{\Pi_j\}}(S|M) \geq 0. \quad (5)$$

Performing projective measurements onto a complete set of orthogonal states of M effectively removes all nonclassical correlations between S and M . In the post-measurement state, mutually orthogonal states of M are correlated with at most as many states of S . It is easy to see that these sorts of correlations can be present in an equivalent classical system.

The value of $\mathcal{J}_{\{\Pi_j\}}(S : M)$ in Eq. (5) depends on the choice of $\{\Pi_j\}$. We want $\mathcal{J}_{\{\Pi_j\}}(S : M)$ to quantify *all* the classical correlations in ρ_{SM} , so we maximize $\mathcal{J}_{\{\Pi_j\}}(S : M)$ over all $\{\Pi_j\}$ and define a measurement-independent mutual information

$$\mathcal{J}(S : M) \equiv H(S) - \tilde{H}(S|M) \geq 0, \quad (6)$$

where

$$\tilde{H}(S|M) \equiv \min_{\{\Pi_j\}} \sum_j p_j H(\rho_{S|j}) \quad (7)$$

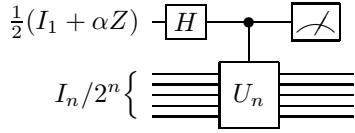
is a measurement-independent conditional information. The quantum discord is then defined as

$$\begin{aligned} \mathcal{D}(S, M) &\equiv \mathcal{I}(S : M) - \mathcal{J}(S : M) \\ &= H(M) - H(S, M) + \tilde{H}(S|M) \\ &= \tilde{H}(S|M) - H(S|M). \end{aligned} \quad (8)$$

The discord is nonnegative and is zero for states with only classical correlations [12, 13]. Thus a nonzero value of $\mathcal{D}(S, M)$ indicates the presence of nonclassical correlations [13]. The discord is bounded above by the marginal entropy $H(M)$ [15].

When the joint state ρ_{SM} is pure, $H(S, M)$ and $\tilde{H}(S|M)$ are zero, $H(S) = H(M) = -H(S|M)$, and the discord is equal to $H(M)$, which is a measure of entanglement for bipartite pure states. In other words, for pure states all nonclassical correlations characterized by quantum discord can be identified as entanglement as measured by the marginal entropy.

So far we have seen how discord can be used to characterize the nonclassical nature of the correlations in quantum states. We now apply these ideas to the DQC1 or *power-of-one-qubit* model [11] of mixed-state quantum computation, which accomplishes the task of evaluating the normalized trace of a unitary matrix efficiently. The quantum circuit corresponding to this model has a collection of n qubits in the completely mixed state, $I_n/2^n$, coupled to a single pure control qubit. A generalized version of this quantum circuit, with the control qubit having sub-unity polarization, is shown below:



This circuit evaluates the normalized trace of U_n , $\tau = \text{Tr}(U_n)/2^n$, with a polynomial overhead going as $1/\alpha^2$.

The problem of evaluating τ is believed to be hard classically. Quantum mechanically, the circuit provides an estimate of τ up to a constant accuracy in a number of trials that does not scale exponentially with n . It does so by making X and Y measurements on the top qubit. The averages of the obtained binary values provide estimates for $\tau_R \equiv \text{Re}(\tau)$ and $\tau_I \equiv \text{Im}(\tau)$. The top qubit is completely separable from the bottom mixed qubits at all times. The final state has vanishingly small entanglement, as measured by the negativity [16] across any split that groups the top qubit with some of the mixed qubits. Nonetheless, there is evidence that the quantum computation performed by this model cannot be simulated efficiently using classical computation [9].

The DQC1 circuit transforms the highly-mixed initial state $\rho_0 \equiv |0\rangle\langle 0| \otimes I_n/2^n$ into the final state ρ_{n+1} ,

$$\begin{aligned} \rho_{n+1} &= \frac{1}{2^{n+1}} \left(|0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes I_n \right. \\ &\quad \left. + \alpha|0\rangle\langle 1| \otimes U_n^\dagger + \alpha|1\rangle\langle 0| \otimes U_n \right) \\ &= \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n^\dagger \\ \alpha U_n & I_n \end{pmatrix}. \end{aligned} \quad (9)$$

Everything about the DQC1 setup, including the measurements on the control qubit, suggests a bipartite split between the control qubit M and the mixed qubits S . Relative to this split, we turn to computing the quantum discord for the state $\rho_{SM} = \rho_{n+1}$. The joint state ρ_{n+1} has eigenvalue spectrum

$$\vec{\lambda}(\rho_{n+1}) = \frac{1}{2^{n+1}} \underbrace{(1 - \alpha, \dots, 1 - \alpha)}_{2^n \text{times}}, \underbrace{(1 + \alpha, \dots, 1 + \alpha)}_{2^n \text{times}}, \quad (10)$$

which gives a joint entropy

$$H(S, M) = n + H_2\left(\frac{1 - \alpha}{2}\right). \quad (11)$$

The marginal density matrix for the control qubit at the end of the computation is

$$\rho_M = \frac{1}{2} \begin{pmatrix} 1 & \alpha \tau^* \\ \alpha \tau & 1 \end{pmatrix}, \quad (12)$$

which has eigenvalues $(1 \pm \alpha|\tau|)/2$ and entropy

$$H(M) = H_2\left(\frac{1 - \alpha|\tau|}{2}\right), \quad (13)$$

where $H_2(\cdot)$ is the binary Shannon entropy.

The evaluation of the quantum conditional entropy involves a minimization over all possible one-qubit projective measurements. The projectors are given by $\Pi_{\pm} = \frac{1}{2}(I_1 \pm \mathbf{a} \cdot \boldsymbol{\sigma})$, with $\mathbf{a} \cdot \mathbf{a} = a_1^2 + a_2^2 + a_3^2 = 1$. The post-measurement states are

$$\rho_{S|\pm} = \frac{1}{p_{\pm} 2^{n+1}} \left(I_n \pm \alpha \frac{a_1 - ia_2}{2} U_n \pm \alpha \frac{a_1 + ia_2}{2} U_n^\dagger \right), \quad (14)$$

occurring with outcome probabilities

$$p_{\pm} = \frac{1}{2}[1 \pm \alpha(a_1 \tau_R + a_2 \tau_I)]. \quad (15)$$

The post-measurement states are independent of a_3 , so without loss of generality, we can let $a_3 = 0$, $a_1 = \cos \phi$, and $a_2 = \sin \phi$. The corresponding post-measurement states are

$$\rho_{S|\pm} = \frac{1}{p_{\pm} 2^{n+1}} \left(I_n \pm \alpha \frac{e^{-i\phi} U_n + e^{i\phi} U_n^\dagger}{2} \right), \quad (16)$$

To find the discord of the state at the end of the computation, we need the spectrum of $\rho_{S|\pm}$ so that we can compute $H(\rho_{S|\pm})$. The eigenvalues of any unitary operator U_n are phases of the form $e^{i\theta_k}$, so we have

$$\lambda_k \left(\frac{e^{-i\phi} U_n + e^{i\phi} U_n^\dagger}{2} \right) = \cos(\theta_k - \phi), \quad k = 1, \dots, 2^n, \quad (17)$$

and

$$\lambda_k(\rho_{S|\pm}) = \frac{1}{2^n} \frac{1 \pm \alpha \cos(\theta_k - \phi)}{1 \pm \alpha(\tau_R \cos \phi + \tau_I \sin \phi)} \equiv q_{k\pm}. \quad (18)$$

We also have

$$\tau_R = \frac{1}{2^n} \sum_k \cos \theta_k \quad \text{and} \quad \tau_I = \frac{1}{2^n} \sum_k \sin \theta_k. \quad (19)$$

All this gives $H(\rho_{S|\pm}) = H(\vec{q}_{\pm})$ and thus

$$\begin{aligned} \tilde{H}_{\Pi_{\pm}} &= p_+ H(\rho_{S|+}) + p_- H(\rho_{S|-}) \\ &= \frac{1}{2}[H(\vec{q}_+) + H(\vec{q}_-)] \\ &\quad + \frac{\alpha}{2}(\tau_R \cos \phi + \tau_I \sin \phi)[H(\vec{q}_+) - H(\vec{q}_-)]. \end{aligned} \quad (20)$$

We now use the fact that we are interested in the behavior of the quantum discord of the DQC1 state for a typical unitary. By typical, we mean a unitary chosen randomly according to the (left and right invariant) Haar measure on $\mathbb{U}(2^n)$. For such a unitary, it is known that the phases θ_k are almost uniformly distributed on the unit circle with large probability [17]. Thus for typical unitaries $\sum_k e^{i\theta_k}$ is close to zero. Hence both τ_R and τ_I are small, and we can ignore the second term on the right-hand side in Eq. (20). In addition, the phases θ_k can be taken to be placed at (with large probability) the 2^n -th roots of unity, i.e., $\theta_k = 2\pi k/2^n$. It follows that the spectra $\lambda_k(\rho_{S|\pm})$ are independent of ϕ . Hence the entropies we are interested in computing are also independent of ϕ , and we can set ϕ to zero without loss of generality. This choice for ϕ corresponds to measuring the pure qubit M along X . The X measurement gives the real part of the normalized trace of U_n , and it is one of the two measurements discussed in the original proposal by Knill and Laflamme. Setting $\phi = \pi/2$ yields the other measurement, along Y , which gives the imaginary part of the normalized trace of U_n .

In the limit of large n , we can simplify Eq. (20) as follows:

$$\begin{aligned} \tilde{H} &= \frac{1}{2}[H(\vec{q}_+) + H(\vec{q}_-)] \\ &= -\frac{1}{2^{n+1}} \sum_{k=1}^{2^n} \left[(1 + \alpha \cos \theta_k) \log \left(\frac{1 + \alpha \cos \theta_k}{2^n} \right) \right. \\ &\quad \left. + (1 - \alpha \cos \theta_k) \log \left(\frac{1 - \alpha \cos \theta_k}{2^n} \right) \right] \\ &= n - \frac{1}{2^{n+1}} \sum_{k=1}^{2^n} \left[\log(1 - \alpha^2 \cos^2 \theta_k) \right. \\ &\quad \left. + \alpha \cos \theta_k \log \left(\frac{1 + \alpha \cos \theta_k}{1 - \alpha \cos \theta_k} \right) \right]. \end{aligned} \quad (21)$$

Furthermore, when n is large, we can replace the sum in the above equation with an integral to obtain

$$\begin{aligned} \tilde{H} &= n - \frac{1}{4\pi} \left[\int_0^{2\pi} \log(1 - \alpha^2 \cos^2 x) dx \right. \\ &\quad \left. + \alpha \int_0^{2\pi} \cos x \log \left(\frac{1 + \alpha \cos x}{1 - \alpha \cos x} \right) dx \right] \\ &= n + 1 - \log \left(1 + \sqrt{1 - \alpha^2} \right) \\ &\quad - \left(1 - \sqrt{1 - \alpha^2} \right) \log e. \end{aligned} \quad (22)$$

Note that when the sums are replaced by integrals, $H(\vec{q}_+) - H(\vec{q}_-) = 0$, providing further justification for ignoring the second term in Eq. (20).

When $|\tau|$ is small, $H(M) \simeq 1$, and the quantum discord for the DQC1 state is then given by the simple expression

$$\begin{aligned} \mathcal{D}_{\text{DQC1}} &= 2 - H_2\left(\frac{1 - \alpha}{2}\right) - \log \left(1 + \sqrt{1 - \alpha^2} \right) \\ &\quad - \left(1 - \sqrt{1 - \alpha^2} \right) \log e. \end{aligned} \quad (23)$$

Figure 1 compares the discord from Eq. (23) with the average discord in a DQC1 circuit having five qubits in the mixed state ($n = 5$) coupled to a control qubit with purity α . The average is taken over 500 instances of pseudo-random unitary matrices. We see that in spite of the approximations made in obtaining Eq. (23), the analytic expression provides a very good estimate of the discord even when n is as low as five.

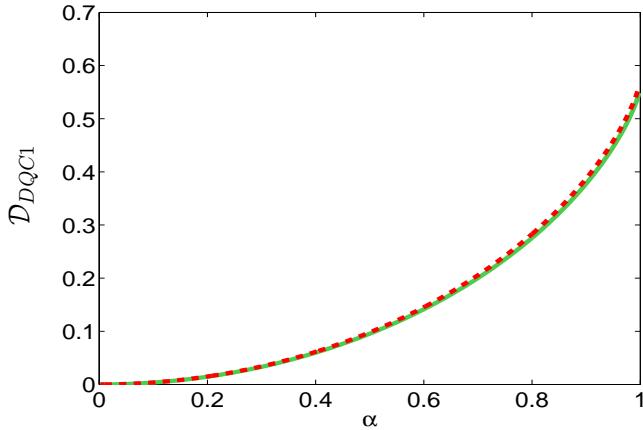


FIG. 1: (Color online) The dashed (red) line shows the average discord in a DQC1 circuit with five qubits in the mixed state ($n = 5$) coupled to a qubit with purity α . The average is taken over five hundred instances of pseudo-random unitary matrices. The discord is shown as a function of the purity of the control qubit. The solid (green) line shows the analytical expression in Eq. (23), which grows monotonically from 0 at $\alpha = 0$ (completely mixed control qubit) to $2 - \log e = 0.5573$ at $\alpha = 1$ (pure control qubit). Even for $n = 5$ the analytical expression is quite accurate. These values of discord should be compared with a maximum possible discord of 1 when M is a single qubit.

There is no entanglement between the control qubit and the mixed qubits in the DQC1 circuit at any point in the computation, yet there are nonclassical correlations, as measured by the discord, between the two parts at the end of the computation for any $\alpha > 0$. Other bipartite splittings of ρ_{n+1} can exhibit entanglement, but it was shown in [16] that the partial transpose criterion failed to detect entanglement in ρ_{n+1} for $\alpha \leq 1/2$. In this domain, several other tests for entanglement, including the first level of the scheme of Doherty *et al.* [18], which is based on semi-definite programming, also failed to detect entanglement. The above expression is thus the first signature of nonclassical correlations in the DQC1 circuit for $\alpha \leq 1/2$.

In conclusion, we calculated the discord in the DQC1 circuit and showed that nonclassical correlations are present in the state at the end of the computation even if there is no detectable entanglement. This shows that for some purposes quantum discord might be a better figure of merit for characterizing the quantum resources available to a quantum information processor. We present evidence of the presence of

nonclassical correlations in the DQC1 circuit when $\alpha \leq 1/2$. The quantum discord for qubits is known to be a true measure of nonclassical correlations [19]. This suggests that nonclassical correlations other than entanglement, as quantified by the discord, may explain the (sometimes exponential) speed-up in the DQC1 circuit and perhaps the speedup in other quantum computational circuits also. For pure states, discord becomes a measure of entanglement. Therefore, using discord to connect quantum resources to the advantages offered by quantum information processors has the additional advantage that it works well for both pure- and mixed-state quantum computation.

We thank W. H. Zurek, C. Rodriguez, and K. Modi for useful discussions on quantum discord. This work was supported in part by Office of Naval Research Contract No. N00014-07-1-0304 and National Science Foundation Grant No. PHY-0653596.

* Electronic address: animesh@unm.edu

† Electronic address: shaji@unm.edu

- [1] A. Ekert and R. Jozsa, Philos. Trans. R. Soc. London A **356**, 1769 (1998).
- [2] R. Jozsa and N. Linden, Proc. Roy. Soc. A **459**, 2011 (2003).
- [3] V. M. Kendon and W. J. Munro, Quantum Inform. Comput. **6**, 630 (2006).
- [4] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
- [5] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
- [6] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
- [7] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, Theor. Comput. Sci. **320**, 15 (2004).
- [8] D. Kenigsberg, T. Mor, and G. Ratsaby, Quantum Inform. Comput. **6**, 606 (2006).
- [9] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
- [10] D. A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
- [11] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
- [12] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
- [13] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2002).
- [14] N. J. Cerf and C. Adami, Phys. Rev. A **60**, 893 (1999).
- [15] The eigendecomposition $\rho_{SM} = \sum_a p_a \Pi_a$ yields $p_j \rho_{S|j} = \sum_a p_a p_{j|a} \rho_{S|a,j}$, where $\rho_{S|a,j} = \text{Tr}_M(\Pi_j \Pi_a)/p_{j|a}$ is a pure state of S . It follows from the pure-state decomposition $\rho_{S|j} = \sum_a p_{a|j} \rho_{S|a,j}$ that $H(A|j) \geq S(\rho_{S|j})$. Thus $H(S, M) = H(A) \geq H(A|J) = \sum_j p_j H(A|j) \geq \tilde{H}_{\{\Pi_j\}}(S|M) \geq \tilde{H}(S|M)$, from which the upper bound on discord follows.
- [16] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
- [17] P. Diaconis, Bull. Amer. Math. Soc. **40**, 155 (2003).
- [18] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
- [19] S. Hamieh, R. Kobes, and H. Zaraket, Phys. Rev. A **70**, 052325 (2004).